

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI**

**JAMES ANDREW CROSSETT,
Individually, and on Behalf of all
Others Similarly Situated,**

Plaintiff,

v.

Civil Action No. 4:17-cv-2434

**CLASS ACTION
JURY TRIAL DEMANDED**

EQUIFAX, INC.,

Defendant.

CLASS ACTION COMPLAINT

COMES NOW Plaintiff JAMES ANDREW CROSSETT (“Plaintiff”), on behalf of himself and all others similarly situated, and brings this action for damages against Equifax, Inc. (“Equifax” or “Defendant”), and alleges, based on information and belief and investigation of counsel as follows:

I. PARTIES, JURISDICTION, AND VENUE

1. Plaintiff is an adult natural person and at all relevant times was a citizen and resident of St. Louis City, Missouri.

2. Plaintiff’s confidential personally identifiable information (“PPI”) was included in the massive data breach of Equifax’s system and disclosed to unauthorized third parties. Plaintiff was thus harmed as a direct and proximate result thereof.

3. Plaintiff is a “consumer” as defined by 15 U.S.C. § 1681a(c).

4. Equifax is a Georgia corporation with its principal place of business in Atlanta, Georgia. Equifax is registered to do business, and is doing business, in the State of Missouri.

Equifax is one of three major credit reporting companies in the United States and is regularly entrusted with the storage and security of PPI.

5. Equifax is a “Consumer Reporting Agency” (“CRA”) as defined by 15 U.S.C. § 1681a(f).

6. Equifax is a “consumer reporting agency that compiles and maintains files on consumers on a nationwide basis” as defined by 15 U.S.C. § 1681a(p).

7. This Court has federal question jurisdiction over this matter under 28 U.S.C. § 1331 as Plaintiffs are bringing claims under the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681e, *et seq.*

8. This Court also has supplemental jurisdiction over all state-law claims pursuant to 28 U.S.C. § 1367.

9. This Court also has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5,000,000.00 exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members. Diversity of citizenship is also present under 28 U.S.C. § 1332(a), as Plaintiff is a citizen of Missouri, Equifax is a citizen of Georgia, and the amount in controversy exceeds \$75,000.00, exclusive of interest and costs.

10. This Court has personal jurisdiction over Equifax because the company regularly conducts business in Missouri and the other 49 states and has sufficient minimum contacts in Missouri. Equifax intentionally avails itself of this jurisdiction by marketing and selling products to millions of consumers nationwide, including in Missouri. Plaintiff’s claims arise from Equifax’s contacts with Missouri.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) and (c) as a substantial part of events or omissions giving rise to the claim occurred in this District and because personal jurisdiction exists over Equifax in this District.

II. GENERAL ALLEGATIONS COMMON TO ALL COUNTS

12. Equifax is in the business of collecting, assessing, storing, and maintaining the information of approximately 800 million worldwide consumers. Equifax collects and stores this information to sell it to third parties in the form of consumer credit reports, insurance reports, and other consumer demographic and analytics information.

13. Equifax also markets and sells credit protection and identity theft monitoring services to the consumers whose personal information Equifax collects.

14. The United States Congress enacted the FCRA to ensure fair and accurate credit reporting, to promote efficiency in the banking system, and to protect consumer privacy.

15. The FCRA requires Consumer Reporting Agencies (CRAs), like Equifax, to protect consumers' privacy by preventing inappropriate disclosure of private information. To comply, CRAs must maintain reasonable procedures to ensure that third-party disclosures are made exclusively for permissible purposes.

16. Given the nature, extent, and sheer volume of sensitive PPI entrusted to it, Equifax was, and is, required to maintain that information in a secure manner and out of the hands of unauthorized individuals and organizations.

17. Equifax is, and has been, aware of the need to maintain the security of such sensitive PPI. For example, Equifax warns of the dangers of identity theft (unauthorized use of sensitive PPI, including for harassment or in the commission of fraud or other criminal acts) and sells credit monitoring services to the very people whose information it maintains.

18. On or about July 29, 2017, Equifax discovered that one or more of its servers, which contained Plaintiffs and Class Members' sensitive personal information including names, full Social Security numbers, birth dates, addresses, and, upon belief, their driver's license numbers and possibly one or more of their credit card numbers, had been breached or "hacked" by a still unknown third party ("July 2017 Breach"). Such information constitutes a "consumer report" as defined by the FCRA because it is information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."

19. The hacking it appears was not sophisticated, but exploited a known vulnerability in software used by Equifax.

20. In early August 2017, before the fact of the July 2017 Breach was made public, multiple Equifax executives sold shares of Equifax stock, worth at least \$1.8 million.

21. Upon information and belief, when Equifax discovered the July 2017 Breach, Equifax immediately began an internal investigation and contracted with an unidentified third-party cybersecurity firm to conduct a review to determine the scope of the hack, including identifying the specific data impacted. That investigation remains ongoing and has yet to be completed.

22. On September 7, 2017, major news outlets began reporting on the July 2017 Breach.

23. These news stories represent the first time that Plaintiffs and all potential Class Members learned that their information secured by Equifax had been compromised. They now live in constant fear that their information is in the hands of criminals.

24. On September 18, 2017, Equifax acknowledged that it became aware of an additional data breach in March of 2017 (March 2017 Breach), unrelated to the July 2017 Breach.

25. According to many security experts, the time period immediately following a data breach is the most opportune time for thieves to exploit the information they have obtained because the victim is unaware that anything has occurred.

26. Equifax's decision to wait six weeks after becoming aware of the July 2017 Breach to inform all consumers was willful and wanton, as well as negligent. By depriving the Plaintiffs and Class Members information about the March 2017 and July 2017 data breaches (collectively referred to as "2017 Data Breaches") in a timely manner, Equifax subjected each consumer to a concrete informational injury, as these consumers were deprived of an opportunity to meaningfully consider and address issues related to the potential fraud, as well as to avail themselves of the remedies available under the FCRA to prevent further dissemination of their private information, including but not limited to the potential remedies under 15 U.S.C. §§ 1681g, 1681c-l, and 1681c-2.

27. In addition to the 2017 Data Breaches, Equifax has been subject to numerous alleged data breaches in the past, yet has failed to enact reasonable procedures to ensure that consumer reports would only be provided for a permissible purpose.

28. The harm to Plaintiff and Class Members was complete at the time the unauthorized breach occurred, as the unauthorized disclosure and dissemination of private credit information causes harm in and of itself.

29. On September 7, 2017, Equifax began to offer consumers like the Plaintiff and Class Members an allegedly dedicated secure website where consumers could determine if their information was compromised (<https://www.equifaxsecurity2017.com>) and offer consumers "free" credit monitoring through an Equifax product, TrustedID Premier (<https://www.equifaxsecurity2017.com/enroll/>), for one year.

30. Under the guise of an effort to mitigate damages and to provide some assistance to the victims of its data breach, including Plaintiff and Class Members, by allowing them "free" access to Defendant's TrustedID Premier service, Defendant, through the terms and conditions of that "free" access, attempted to induce the victims, including Plaintiff and Class Members, to waive their rights to bring or participate in a class action lawsuit and require them to submit to arbitration (<http://www.equifax.com/terms/>) (amended September 12, 2017 to remove the arbitration and class action waiver to the claims alleged herein, only after the urgings of New York Attorney General Eric Schneiderman). This conduct was also intended to deprive the Plaintiff and Class Members of the ability to avail themselves of the remedies available under state and federal laws to obtain compensation for the data breach and prevent further dissemination of their private information.

31. Unlike other data breaches, not all of the people affected by the Equifax July 2017 Data Breach may be aware that they're customers of the company. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records. People affected may not realize that Equifax has their data. Thus, it appears that many people whose data was exposed did not provide that information directly to Equifax and may not even know Equifax had it.

32. As a proximate result of Equifax's failure to secure and safeguard the private information it collects, stores, and sells, the Plaintiff and Class Members' private information was accessed and stolen by hackers.

33. As a further proximate result of Equifax's acts or omissions, the Plaintiff and Class Members have been subjected to an imminent and immediate but continuing and ongoing risk of identity theft and identity fraud.

III. CLASS ALLEGATIONS

34. Plaintiff brings this action on behalf of himself and all others similarly situated as a nationwide class action pursuant to Federal Rule of Civil Procedure 23. The class which Plaintiff seeks to represent (“Class”) is composed of and defined as:

All persons in the United States whose private, personal information was impermissibly released as a result of the July 2017 Data Breach.

35. Excluded from the Class are:

- a. Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors;
- b. the Judge to whom this case is assigned and the Judge's immediate family;
- c. any person who executes and files a timely request for exclusion from the Class;
- d. any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and
- e. the legal representatives, successors and assignees of any such excluded person.

36. This action has been brought and may be properly maintained as a class action and satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements thereof.

37. The putative Class, through information and belief, are comprised of thousands or millions of persons, making joinder impractical. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the parties and the Court.

38. The rights of all Class Members have been violated in an identical, or nearly identical way and questions of law and fact common to the proposed class predominate over any individual questions. Common questions of law and fact include, but are not limited to:

- a. Whether Defendant promulgated, implemented and enforced reasonable procedures to prevent unauthorized access of the Plaintiff and Class Members' private information;
- b. Whether Defendant failed to notify or warn the Plaintiff and Class Members of the July 2017 Data Breach in a reasonable manner, within a reasonable time;
- c. Whether Defendant failed to take reasonable steps to protect consumers it knew, or should have known, were affected by the July 2017 Data Breach;
- d. Whether Equifax acted willfully, negligently, grossly negligently, and/or recklessly with respect to securing Class Members' sensitive private personal information from unauthorized disclosure;
- e. Whether the Plaintiff and Class Members suffered damages as a result of the July 2017 Data Breach;
- f. Whether the Plaintiff and Class Members are entitled to statutory damages; and,
- g. Whether the Plaintiff and Class Members are entitled to punitive damages.

39. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class Members sustained damages arising out of Equifax's common course of conduct in violation of the law as complained herein. The losses of each member of the Class were caused directly by Equifax's wrongful conduct in violation of the law as alleged herein.

40. Plaintiff named herein will fairly and adequately protect the interests of the Class Members. Plaintiff has no interests which are adverse to the interests of absent Class Members. Plaintiff, like all Class Members, suffered an avoidable breach of his confidential PPI.

41. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual joinder of all Class Members is impracticable. Furthermore, because the damages suffered by each individual member of the Class may be relatively small, the expense and burden of individual litigation would make it difficult or impossible for individual Class Members to redress the wrongs done to them. Individual litigation

would likewise burden the court system to a much greater degree than a class action, and would present the potential for inconsistent or contradictory judgments. By contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves the resources of the parties and the court system, and protects the rights of each Class Member.

IV. CLAIMS FOR RELIEF

I. VIOLATION OF THE FAIR CREDIT REPORTING ACT

42. Plaintiff incorporates by reference paragraphs 1-41 of this Complaint as if fully set forth herein.

43. The Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* (“Act”), was designed to require consumer reporting agencies such as Equifax to adopt and maintain procedures for “maintaining the confidentiality ... and proper utilization” of sensitive PPI (including “consumer credit, personnel, insurance, and other information”), among other purposes. 15 U.S.C. § 1681(b); 15 U.S.C. § 1681e(a).

44. The Act strictly limits the purposes and circumstances under which sensitive PPI may be disclosed. 15 U.S.C. § 1681b.

45. Equifax is well informed of and publicizes its obligations and duties concerning the sensitive PPI with which it is entrusted. *See, e.g.,* <http://www.equifax.com/privacy/fcra/>. Equifax is well informed of the steps and precautions necessary to prevent unauthorized access of such information. Equifax is well informed of the consequences of unauthorized disclosure of such information. Equifax holds itself out as one a means of defense and protection to identity theft.

46. On, before, and after July 2017, Equifax did not have in place proper and adequate procedures to limit the disclosure of sensitive PPI (including that of Plaintiff and the Class

Members) to unauthorized individuals or groups for purposes beyond the strict limitations of the Act

47. Equifax failed to ensure that the sensitive PPI of Plaintiffs and the Class Members was not disclosed to unauthorized individuals but instead willfully, recklessly, and/or negligently allowed hackers through unsophisticated methods to obtain such information.

48. Equifax failed to notify the Plaintiff or Class Members regarding the compromise of their PPI and the Plaintiff and Class Members only became aware through media reports weeks after the July 2017 Data Breach.

49. Equifax has violated the Act willfully, recklessly, and/or negligently by allowing hackers to obtain sensitive PPI of Plaintiff and Class Member.

50. As a proximate result of each and every willful violation of the FCRA, Plaintiff and Class Members seek:

- a. Actual damages under 15 U.S.C. § 1681n(a)(1);
- b. Statutory damages under 15 U.S.C. § 1681(a)(1);
- c. Punitive damages under 15 U.S.C. § 1681n(a)(2); and
- d. Reasonable attorney's fees and costs under 15 U.S.C. § 1681n(a)(3).

51. As a proximate result of every negligent violation of the FCRA, Plaintiff and Class Members seek:

- a. Actual damages under 15 U.S.C. § 1681o(a)(1); and
- b. Reasonable attorney's fees and costs under 15 U.S.C. § 1681o(a)(2).

II. NEGLIGENCE AND GROSS NEGLIGENCE

52. Plaintiff incorporates by reference paragraphs 1-51 as if fully set forth herein.

53. Equifax owed a duty of reasonable care in protecting the sensitive PPI of Plaintiff and Class members from unauthorized disclosure.

54. Equifax owed a duty of reasonable care to Plaintiff and Class Members to discover hacking and unauthorized taking of sensitive PPI.

55. Equifax owed a duty of reasonable care to Plaintiff and Class Members to promptly notify them of the unauthorized disclosure of sensitive PPI and to take additional steps to mitigate the harms from the unauthorized disclosure.

56. Plaintiff and the Class Members were foreseeable victims of Equifax's inadequate safety and security practices. Plaintiff and the Class Members had no means of protecting the PPI that was in Equifax's possession.

57. Equifax has admitted that Plaintiff and the Class Members' PPI was wrongfully disclosed as a result of the July 2017 Data Breach. Because the breach was the result of a known website vulnerability, it could easily have been prevented.

58. Equifax breached its duties to Plaintiff and Class Members by failing to maintain proper security measures, policies and procedures, and training.

59. Equifax further breached its duties by failing to timely notify Plaintiff and the Class Members of the July 2017 Data Breach, and waiting weeks from discovery of the hack to publicly disclose it.

60. As a direct and proximate result of Equifax's violations of the Act and common law, Plaintiff and Class Members suffered damages. Damages include, without limitation, time, effort, and expense to take measures to mitigate identity theft and its possibility, including credit freezes, fraud alerts, credit monitoring, and/or identity theft insurance, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

III. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that the Court enter judgment against Equifax and in favor of Plaintiff and the Class Members, and award the following relief:

- (a) following appropriate discovery, an Order certifying this cause as a Class under Federal Rule of Civil Procedure 23 and appointing James Andrew Crossett as class representative and Gori Julian & Associates, P.C. as class counsel.
- (b) actual damages against Equifax for all the allegations contained in Counts I-II;
- (c) punitive damages, as allowed by law, against Equifax for all the allegations contained in Counts I-II;
- (d) statutory damages to Plaintiff and Class Members;
- (e) reasonable attorneys' fees as determined by the Court;
- (f) interest;
- (g) costs; and
- (h) such other further or different relief as the Court may deem appropriate.

Plaintiff demands trial by struck jury on all Counts.

Respectfully submitted,

/s/ D. Todd Mathews
D. Todd Mathews, #52502
Evan D. Buxner, of counsel, #41559
Megan T. Arvola, #65578
Gori Julian & Associates, P.C.
156 N. Main Street
Edwardsville, IL 62025
(618) 659-9833 – Telephone
(618) 659-9834 – Facsimile
todd@gorijulianlaw.com
evan@gorijulianlaw.com
marvola@gorijulianlaw.com